




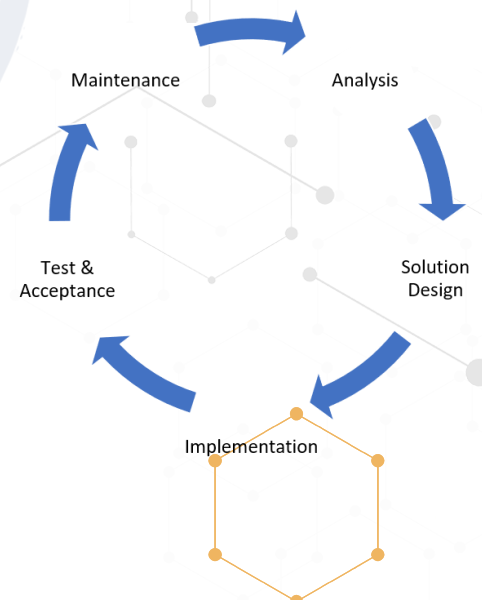
Welcome to the Second Chapter.

➤ Domain 2: What we will be covering.


- **BCP (Business Continuity Plan):**
 - The overarching plan, with many subplans.
 - This is the process of creating the long-term strategic business plans, policies, and procedures for continued operation after a disruptive event.
- **DRP (Disaster Recovery Plan):**
 - Focused on our IT systems.
 - How do we recover fast enough in a disaster scenario.
 - DRP has a lifecycle of Mitigation, Preparation, Response and Recovery.
- **Incident Management:**
 - How we monitor and detect security events on our systems, and how we react in those events.

➤ BCP - Business Continuity Plan:

- **Business Continuity Plan (BCP)** 
 - This is the process of creating the long-term strategic business plans, policies, and procedures for continued operation after a disruptive event.
 - It is for the entire organization, everything that could be impacted, not just IT.
 - Lists a range of disaster scenarios and the steps the organization must take in any particular scenario to return to regular operations.
 - BCPs often contain COOP (Continuity of Operations Plan), Crisis Communications Plan, Critical Infrastructure Protection Plan, Cyber Incident Response Plan, DRP (Disaster Recovery Plan), ISCP (Information System Contingency Plan), Occupant Emergency Plan.
 - We look at what we would do if a critical supplier closed, the facility was hit by an earthquake, what if we were snowed in and staff couldn't get to work, ...
 - They are written ahead of time, and continually improved upon, it is an iterative process.
 - We write the BCP with input from key staff and at times outside BCP consultants.



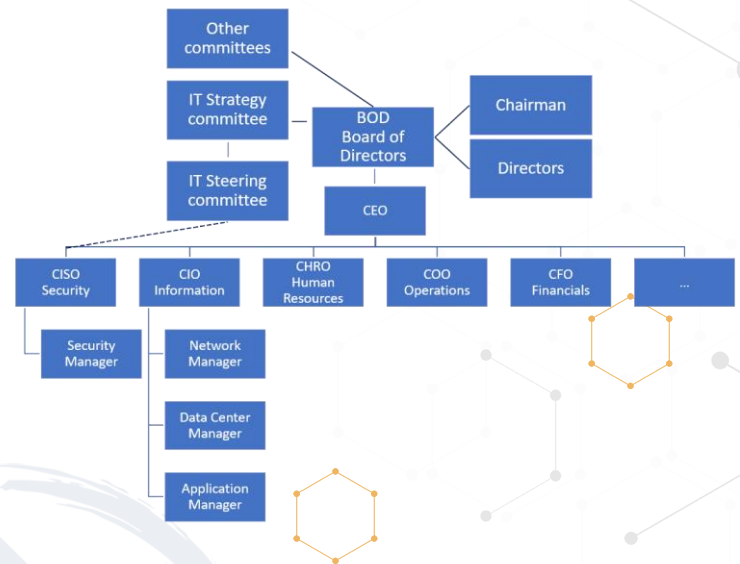


- Senior management needs to be involved and committed to the BCP/DRP process.
- They need to be part of at least the initiation and the final approval of the plans.
 - They are responsible for the plan, they own the plan and since they are ultimately liable, they must show due-care and due-diligence.
 - We need top-down IT security in our organization (the exam assumed we have that).
 - In serious disasters, it will be Senior Management or someone from our legal department who should talk to the press.
 - Most business areas often feel they are the most important area and because of that their systems and facilities should receive the priority, senior management being ultimately liable and the leaders of our organization, obviously have the final say in priorities, implementations, and the plans themselves.
- **Related Plans:** 
 - Our BCP being the overarching plan also contains our other plans, including but not limited to:
 - **COOP (Continuity of Operations Plan):**
 - ♦ How we keep operating in a disaster, how do we get staff to alternate sites, what are all the operational things we need to ensure we function even if at reduced capacity for up to 30 days.
 - **Crisis Communications Plan:**
 - ♦ A subplan of the CMP.
 - ♦ How we communicate internally and externally during a disaster.
 - ♦ Who is permitted to talk to the press? Who is allowed to communicate what to whom internally?
 - **Cyber Incident Response Plan:**
 - ♦ How we respond in cyber events, can be part of the DRP or not. This could be DDOS, worms, viruses,...
 - **OEP (Occupant Emergency Plan):**
 - ♦ How do we protect our facilities, our staff and the environment in a disaster event.
 - ♦ This could be fires, hurricanes, floods, criminal attacks, terrorism,...
 - ♦ Focuses on safety and evacuation, details how we evacuate, how often we do the drills and the training staff should get.
 - **BRP (Business Recovery Plan):**
 - ♦ Lists the steps we need to take to restore normal business operations after recovering from a disruptive event.
 - ♦ This could be switching operations from an alternate site back to a (repaired) primary site.
 - **Continuity of Support Plan:**
 - ♦ Focuses narrowly on support of specific IT systems and applications.
 - ♦ Also called the IT Contingency Plan, emphasizing IT over general business support.

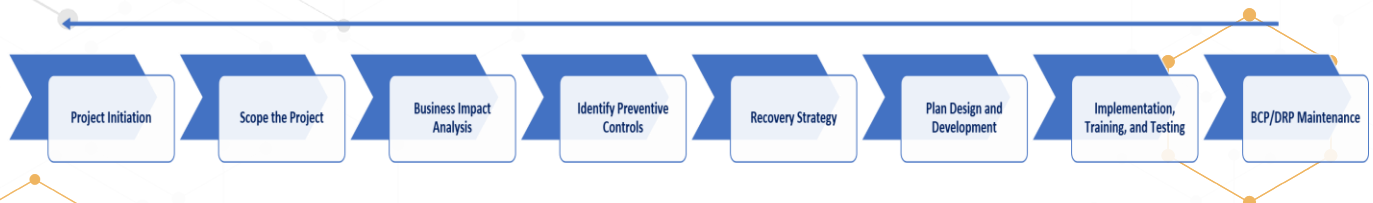


■ CMP (The Crisis Management Plan):

- ♦ Gives us effective coordination among the management of the organization in the event of an emergency or disruptive event.
- ♦ Details what steps management must take to ensure that life and safety of personnel and property are immediately protected in case of a disaster.



- Older versions of NIST 800-34 had these steps as a framework for building our BCP/DRP.
- **Project Initiation:** We start the project, identify stakeholders, get C-level approval and formalize the project structure.
- **Scope the Project:** We identify exactly what we are trying to do and what we are not.
- **Business Impact Analysis:** We identify and prioritize critical systems and components.
- **Identify Preventive Controls:** We identify the current and possible preventative controls we can deploy.
- **Recovery Strategy:** How do we recover efficiently? What are our options? DR site, system restore, cloud,...
- **Plan Design and Development:** We build a specific plan for recovery from a disaster, procedures, guidelines and tools.
- **Implementation, Training, and Testing:** We test the plan to find gaps and we train staff to be able to act on the plan.
- **BCP/DRP Maintenance:** It is an iterative process. Our organization develops, adds systems, facilities or technologies and the threat landscape constantly changes, we have to keep improving and tweaking our BCP and DRP.





- We categorize disasters in 3 categories: **Natural, Human, or Environmental.**
 - **Natural:**
 - ♦ Anything caused by nature, this could be earthquakes, floods, snow, tornados, ...
 - ♦ They can be very devastating but are less common than the other types of threats.
 - ♦ The natural disaster threats are different in different areas, we do the risk analysis on our area.
 - ♦ For one site we could build our buildings and data center earthquake resilient and another flood resilient.
 - **Human:**
 - ♦ Anything caused by humans, they can be intentional or unintentional disasters.
 - ♦ Unintentional could be an employee uses a personal USB stick on a PC at work and spreads malware, just as bad as if an attacker had done it, but the employee was just ignorant, lazy or didn't think it would matter.
 - ♦ Intentional could be malware, terrorism, DOS attacks, hacktivism, phishing, ...
 - **Environmental (Not to be confused with natural disasters):**
 - ♦ Anything in our environment, could be power outage/spikes, hardware failures, provider issues, ...
- The plans need to be continually updated; it is an iterative process.
 - Plans should be reviewed and updated at least every 12 months.
 - We changed major components of our systems (new backup solution, new IP scheme,...).
 - We had a disaster, and we had a lot of gaps in our plans.
 - A significant part of senior leadership has changed.

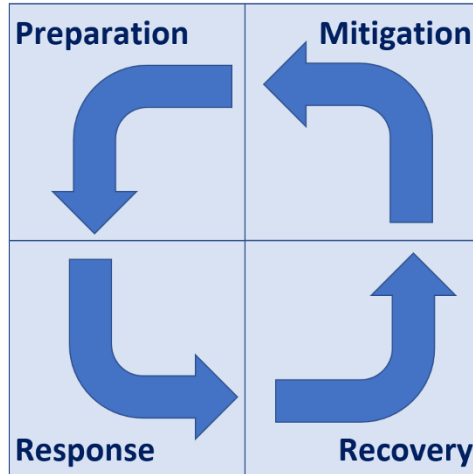
▶ **DRP – Disaster Recovery Plan:**

- Our **DRP (Disaster Recovery Plan)** should answer at least three basic questions:
 - What is the objective and purpose?
 - Who will be the people or teams who will be responsible in case any disruptions happen?
 - What will these people do (our procedures) when the disaster hits?
- **DRP has a lifecycle of Mitigation, Preparation, Response and Recovery.**
 - **Mitigation:** Reduce the impact, and likeliness of a disaster.
 - **Preparation:** Build programs, procedures and tools for our response.





Education,
Plans,
Processes &
Training.

DR/BCP/EOP
(emergency
Operations
plan)




Pre-disaster
mitigation
implementations.




Post-disaster
recovery plan.

- In our recovery process we have to consider the many factors that can impact us, we need look at our options if our suppliers, contractors or the infrastructure are impacted as well.
- We may be able to get our data center up and running in 12 hours, but if we have no outside connectivity that may not matter.
- **Simulated Tests:** 
 - **DRP Review:**
 - ♦ Team members who are part of the DRP team review the plan quickly looking for glaring omissions, gaps or missing sections in the plan.
 - **Read-Through (Checklist):**
 - ♦ Managers and functional areas go through the plan and check a list of components needed for in the recovery process.
 - **Walk/Talk-through (Tabletop or Structured Walkthrough):**
 - ♦ A group of managers and critical personnel sit down and talk through the recovery process.
 - ♦ Can often expose gaps, omissions or just technical inaccuracies that would prevent the recovery.
 - **Simulation Test (Walkthrough Drill):**
 - ♦ Similar to the walkthrough (but different, do not confuse them).
 - ♦ The team simulates a disaster and the teams respond with their pieces from the DRP.
- **Physical Tests:** 
 - **Partial Interruption:**
 - ♦ We interrupt a single application and fail it over to our secondary facilities, often done off hours.



- We have looked at the first 2 before, for now we will focus on Response and Recovery.
 - **Response:** How we react in a disaster, following the procedures.
 - ♦ How we respond and how quickly we respond is essential in Disaster Recovery.
 - ♦ We assess if the incident we were alerted to or discovered is serious and could be a disaster, the assessment is an iterative process.
 - ♦ The more we learn and as the team gets involved we can assess the disaster better.
 - ♦ We notify appropriate staff to help with the incident (often a call tree or automated calls), inform the senior management identified in our plans and if indicated by the plan communicate with any other appropriate staff.
 - **Recovery:** Reestablish basic functionality and get back to full production.
 - ♦ We act on our assessment using the plan.
 - ♦ At this point all key stakeholders should be involved, we have a clearer picture of the disaster and take the appropriate steps to recover. This could be DR site, system rebuilds, traffic redirects,...
- **BIA (Business Impact Analysis):** 
 - Identifies critical and non-critical organization systems, functions, and activities.
 - Critical is where disruption is considered unacceptable, the acceptability is also based on the cost of recovery.
 - A function may also be considered critical if dictated by law.
 - For each critical (in scope) system, function, or activity, two values are then assigned:
 - **RPO (Recovery Point Objective):** The acceptable amount of data that can not be recovered.
 - ♦ The recovery point objective must ensure that the maximum tolerable data loss for each system, function or activity is not exceeded.
 - ♦ If we only back up once a week, we accept up to a week of data loss.
 - **MTD (Maximum Tolerable Downtime) $MTD \geq RTO + WRT$:**
 - ♦ The time to rebuild the system and configure it for reinsertion into production must be less than or equal to our MTD.
 - ♦ The total time a system can be inoperable before our organization is severely impacted.
 - ♦ Remember companies that had a major loss of data, 43% never reopen and 29% close within two years.
 - ♦ Other frameworks may use other terms for MTD, but for the exam know and use MTD.
 - ♦ MAD (Maximum Allowable Downtime), MTO (Maximum Tolerable Outage), MAO (Maximum Acceptable Outage), MTPoD (Maximum Tolerable Period of Disruption).
 - **RTO (Recovery Time Objective):** The amount of time to restore the system (hardware).



- ♦ The recovery time objective must ensure that the MTD for each system, function or activity is not exceeded.
- **WRT (Work Recovery Time) (software):**
 - ♦ How much time is required to configure a recovered system.
- **MTBF (Mean Time Between Failures):**
 - ♦ How long a new or repaired system or component will function on average before failing, this can help us plan for spares and give us an idea of how often we can expect hardware to fail.
- **MTTR (Mean Time to Repair):**
 - ♦ How long it will take to recover a failed system.
- **MOR (Minimum Operating Requirements):**
 - ♦ The minimum environmental and connectivity requirements for our critical systems to function, can also at times have minimum system requirements for DR sites.
 - ♦ We may not need a fully spec'd system to resume the business functionality.
- **Recovery Strategies:**
 - From our MTD we can determine our approach to how we handle disasters and the safeguards we put in place to mitigate or recover from them.
 - **Redundant Site:**
 - ♦ Complete identical site to our production, receives a real time copy of our data.
 - ♦ Power, HVAC, Raised floors, generators,...
 - ♦ If our main site is down the redundant site will automatically have all traffic fail over to the redundant site.
 - ♦ The redundant site should be geographically distant, and have staff at it.
 - ♦ By far the most expensive recovery option, end users will never notice the fail over.
 - **Hot Site:**
 - ♦ Similar to the redundant site, but only houses critical applications and systems, often on lower spec'd systems.
 - ♦ Still often a smaller but a full data center, with redundant UPS's, HVAC's, ISP's, generators,...
 - ♦ We may have to manually fail traffic over, but a full switch can take an hour or less.
 - ♦ Near or real-time copies of data.
 - **Warm Site:**
 - ♦ Similar to the hot site, but not with real or near-real time data, often restored with backups.
 - ♦ A smaller but full data center, with redundant UPS's, HVAC's, ISP's, generators,...
 - ♦ We manually fail traffic over, a full switch and restore can take 4-24+ hrs.



▪ Cold Site:



- ♦ A smaller but full data center, with redundant UPSs', HVAC's, ISP's, generators,...
- ♦ No hardware or backups are at the cold site, they require systems to be acquired, configured and applications loaded and configured.
- ♦ This is by far the cheapest, but also longest recovery option, can be weeks+.

▪ Reciprocal Agreement Site:



- ♦ Your organization has a contract with another organization that they will give you space in their data center in a disaster event and vice versa.
- ♦ This can be promised space or some racks with hardware completely segmented off the network there.

▪ Subscription/Cloud Site:



- ♦ We pay someone else to have a minimal or full replica of our production environment up and running within a certain number of hours (SLA).
- ♦ They have fully built systems with our applications and receive backups of our data, if we are completely down we contact them and they spin the systems up and apply the latest backups.
- ♦ How fast and how much is determined by our plans and how much we want to pay for this type of insurance.

Site	Cost	Hardware/Equipment	Telecommunications	Setup Time	Location
Cold Site	Low	None	None	Long	Fixed
Warm Site	Medium	Partial	Partial/Full	Medium	Fixed
Hot Site	Medium/ High	Full	Full	Short	Fixed
Mobile Site	High	Dependent	Dependent	Dependent	Not Fixed
Mirrored Site	High	Full	Full	None	Fixed

▪ Mobile Site:

- ♦ Basically a data center on wheels, often a container or trailer that can be moved wherever by a truck.
- ♦ Has HVAC, fire suppression, physical security, (generator),... everything you need in a full data center.
- ♦ Some are independent with generator and satellite internet, others need power and internet hookups.

- Once we have had and recovered from a disruption or we have done our failover test we do a lessons learned.

• Lessons Learned:

- This phase is often overlooked, we removed the problem, we have implemented new controls and safeguards.
- We can learn a lot from lessons learned, not just about the specific incidence, but how well we handle them, what worked, what didn't.




- What happened and didn't happen is less important than how we improve for next time.
- We do not place blame, the purpose is improving.
- How can we as an organization grow and become better next time we have another incidence? While we may have fixed this one vulnerability there are potentially 100's of new ones we know nothing about yet.
- The outcome and changes of the Lessons Learned will then feed into our preparation and improvement of our BCP and DRP.
- We only use our BCP/DRP's when our other countermeasures have failed.
- This makes the plans even more important. **(Remember 72% of business with major data loss closed).**
- When we make and maintain the plans there are some common pitfalls we want to avoid:
 - Lack of senior leadership support
 - Too narrow scope
 - Not keeping the BCP/DRP plans up to date, or no proper versioning controls
- The plans need to be continually updated, it is an iterative process.
 - Plans should be reviewed and updated at least every 12 months.
 - When we update the plans older copies are retrieved and destroyed, and current versions are distributed.

► Incident Management:

- **Incident Management:**
 - Involves the monitoring and detection of security events on our systems, and how we react in those events.
 - It is an administrative function of managing and protecting computer assets, networks, and information systems.
 - The primary purpose is to have a well understood and predictable response to events and computer intrusions.
 - We have very clear processes and responses, and our teams are trained in them and know what to do when an event occurs.
 - Incidents are very stressful situations, it is important staff knows exactly what to do, that they have received ongoing training and understand the procedures.
- **We categorize disasters in 3 categories: Natural, Human, or Environmental.**
 - **Natural:**
 - ♦ Anything caused by nature, this could be earthquakes, floods, snow, tornados, ...
 - ♦ They can be very devastating, but are less common than the other types of threats.
 - ♦ The natural disaster threats are different in different areas, we do the risk analysis on our area.



- ♦ For one site we could build our buildings and data center earthquake resilient and another flood resilient.
- **Human:**
 - ♦ Anything caused by humans, they can be intentional or unintentional disasters.
 - ♦ Unintentional could be an employee uses a personal USB stick on a PC at work and spreads malware, just as bad as if an attacker had done it, but the employee were just ignorant, lazy or didn't think it would matter.
 - ♦ Intentional could be malware, terrorism, DOS attacks, hacktivism, phishing, ...
- **Environmental (Not to be confused with natural disasters):**
 - ♦ Anything in our environment, could be power outage/spikes, hardware failures, provider issues, ...
- **Incident Management:** 
 - **Event:**
 - ♦ An observable change in state, this is neither negative nor positive, it is just something has changed.
 - ♦ A system powered on, traffic from one segment to another, an application started.
 - **Alert:**
 - ♦ Triggers warnings if certain event happens.
 - ♦ This can be traffic utilization above 75% or memory usage at 90% or more for more than 2 minutes.
 - **Incident:**
 - ♦ **Multiple adverse** events happening on our systems or network, often caused by people.
 - **Problem:**
 - ♦ Incidence with an unknown cause, we would follow similar steps to incidence response.
 - ♦ More time would be spent on root cause analysis, we need to know what happened so we can prevent it from happening again, this could be a total internet outage or server crash.
 - **Inconvenience (Non-disasters):**
 - ♦ Non-disruptive failures, hard disk failure, 1 server in a cluster is down,...
 - **Emergency (Crisis):**
 - ♦ Urgent, event with the potential for loss of life or property.
 - **Disaster:**
 - ♦ Our entire facility is unusable for 24 hours or longer.
 - ♦ If we are geographically diverse and redundant we can mitigate this a lot.
 - ♦ Yes, a snowstorm can be a disaster.
 - **Catastrophe:**
 - ♦ Our facility is destroyed



- **NIST 800-61 - IR lifecycle** (ALL NIST publications are free)
 - <https://thorteaches.com/study/> -> Scroll down to free stuff.
- **CIRT (Cyber Incident Response Team):**
 - Senior management
 - Incident manager
 - Technical leads and teams.
 - IT Security.
 - PR, HR, and legal.
 - Auditors IT/financial.

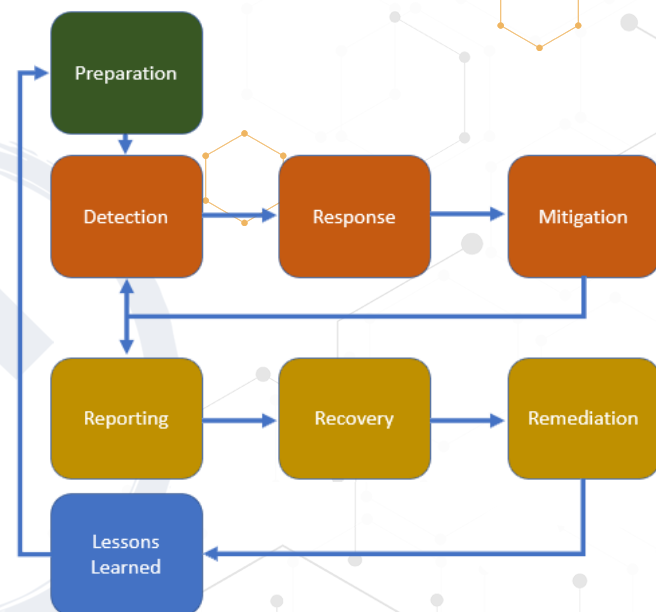
- **Incident Management:**
 - We most common use a 8-step lifecycle.
 1. **Preparation.**
 2. **Detection**
 3. **Response**
 4. **Mitigation**
 5. **Reporting.**
 6. **Recovery.**
 7. **Remediation.**
 8. **Lessons Learned**

- **Preparation:**

- ♦ This is all the steps we take to prepare for incidences.
- ♦ We write the policies, procedures, we train our staff, we procure the detection soft/hardware, we give our incidence response team the tools they need to respond to an incident.
- ♦ The more we train our team, the better they will handle the response, the faster we recover, the better we preserve the crime scene (if there is one), the less impactful an incident will be.

- **Detection:**

- ♦ Events are analyzed to determine if they might be a security incident.
- ♦ If we do not have strong detective capabilities in and around our systems, we will most likely not realize we have a problem until long after it has happened.
- ♦ The earlier we detect the events, the earlier we can respond, IDS's can help us detect, where IPS's can help us detect and prevent further compromise.
- ♦ The IDS's and IPS's can help us detect and prevent on a single network segment, we also need something that can correlate all the information from the entire network.





▪ Response:

- ♦ The response phase is when the incident response team begins interacting with affected systems and attempts to keep further damage from occurring as a result of the incident.
- ♦ This can be taking a system off the network, isolating traffic, powering off the system, or however our plan dictates to isolate the system to minimize both the scope and severity of the incident.
- ♦ Knowing how to respond, when to follow the policies and procedures to the letter and when not to, is why we have senior staff handle the responses.
- ♦ We make bit level copies of the systems, as close as possible to the time of incidence to ensure they are a true representation of the incident.
- ♦ IT Security is there to help the business, it may not be the choice of senior management to disrupt business to contain or analyze, it is ultimately a decision that is made by them.
- ♦ We stop it from spreading, but that is it, we contain the event.


▪ Mitigation:

- ♦ We understand the cause of the incident so that the system can be reliably cleaned and restored to operational status later in the recovery phase.
- ♦ Organizations often remove the most obvious sign of intrusion on a system or systems, but miss backdoors and other malware installed in the attack.
- ♦ The obvious sign is often left to be found, where the actual payload is hidden. If that is detected or assumed, we often just rebuild the system from scratch and restore application files from a known good backup, but not system files.
- ♦ To ensure the backup is good, we need to do root cause analysis, we need a timeline for the intrusion, when did it start?
- ♦ If it is from a known vulnerability we patch. If it's a newly discovered vulnerability we mitigate it before exposing the newly built system to the outside again.
- ♦ If anything else can be learned about the attack, we can add that to our posture.
- ♦ Once eradication is complete, we start the recovery phase.

▪ Reporting:

- ♦ We report throughout the process beginning with the detection, and we start reporting immediately when we detect malicious activity.
- ♦ The reporting has 2 focus areas: technical and non-technical.
- ♦ The incident handling teams report the technical details of the incident as they start the incident handling process, but they also notify management of serious incidents.
- ♦ The procedures and policies will outline when which level of management needs to be informed and involved, it is commonly forgotten until later and can be a RPE (Resume Producing Event).



- ♦ Management will also involve other departments if needed, this could be legal, PR or whomever has been identified in the policies or procedures.
- **Recovery:**
 - ♦ We carefully restore the system or systems to operational status.
 - ♦ When the system is ready for reinsertion is determined by the business unit responsible for the system.
 - ♦ We closely monitor the rebuilt or cleaned system carefully, it is possible the attackers left backdoors or we did not remove all the infected sectors.
 - ♦ Often the system(s) are reinserted off peak hours to minimize the effect of the system(s) still being infected, or they can be introduced in a controlled sandbox environment to see if the infection persists.
- **Remediation:**
 - ♦ The remediation happens during the mitigation phase, where vulnerabilities on the impacted system or systems are mitigated.
 - ♦ Remediation continues after mitigation and becomes broader, this can be patching all systems with the same vulnerability or change how the organization authenticates.
- **Lessons Learned:** 
 - ♦ This phase is often overlooked, we removed the problem, we have implemented new controls and safeguards.
 - ♦ We can learn a lot from lessons learned, not just about the specific incidence, but how well we handle them, what worked, what didn't.
 - ♦ How can we as an organization grow and become better next time we have another incidence? While we may have fixed this one vulnerability there are potentially 100's of new ones we know nothing about yet.
 - ♦ At the end of lessons learned we produce a report to senior management, with our findings, we can only make suggestions, they are ultimately in charge (and liable).
 - ♦ Often after major incidents organizations shift to a top-down approach and will listen more to IT Security.
 - ♦ The outcome and changes of the Lessons Learned will then feed into our preparation.
- **Root-Cause Analysis:**
 - ♦ We attempt to determine the underlying weakness or vulnerability that allowed the incident to happen.
 - ♦ If we do not do the root-cause analysis we will most likely face the same problem again.
 - ♦ We need to fix the vulnerability on the system(s) that were effected, but also on any system in the organization that has that particular vulnerability or set of vulnerabilities.
 - ♦ We could have a weak password policy and weak encryption, that could be the root cause of a system compromise, we then would implement countermeasures to remove the vulnerability.

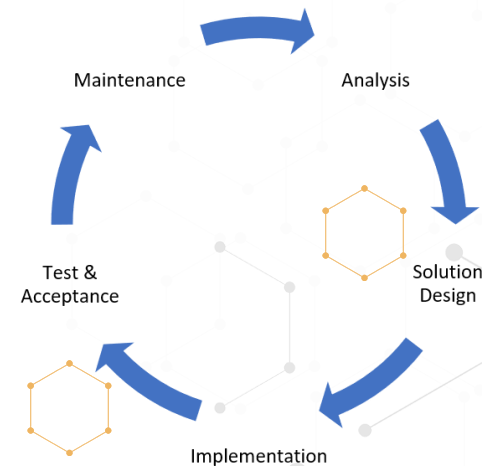


- ♦ If we do nothing and just fix the problem, the root of the issue still persists, that is what we need to fix.

- **BCP (Business Continuity Plan):**



- This is the process of creating the long-term strategic business plans, policies and procedures for continued operation after a disruptive event.
- It is for the entire organization, everything that could be impacted, not just IT.
- Lists a range of disaster scenarios and the steps the organization must take in any particular scenario to return to regular operations.
- BCP's often contain COOP (Continuity of Operations Plan), Crisis Communications Plan, Critical Infrastructure Protection Plan, Cyber Incident Response Plan, DRP (Disaster Recovery Plan), ISCP (Information System Contingency Plan), Occupant Emergency Plan.
- What would we do if a critical supplier closed, the facility was hit by an earthquake, what if we were snowed in and staff couldn't get to work,...
- They are written ahead of time, and continually improved upon, it is an iterative process.
- We write the BCP with input from key staff and at times outside BCP consultants.



- **DRP (Disaster Recovery Plan):**

- This is the process of creating the short-term plans, policies, procedures and tools to enable the recovery or continuation of vital IT systems in a disaster.
- It focuses on the IT systems supporting critical business functions, and how we get those back up after a disaster.
- DRP is a subset of our BCP.
- We look at what we would do if we get hit with a DDOS attack (can be in the DRP or in our Cyber Incident Response Plan), a server gets compromised, we experience a power outage, ...
- Often the how and system specific, where the BCP is more what and non-system specific.

- **We categorize disasters in 3 categories: Natural, Human, or Environmental.**

- **Natural:**

- ♦ Anything caused by nature, this could be earthquakes, floods, snow, tornados, ...
- ♦ They can be very devastating, but are less common than the other types of threats.



- ♦ The natural disaster threats are different in different areas, we do the risk analysis on our area.
- ♦ For one site we could build our buildings and data center earthquake resilient and another flood resilient.
- **Human:**
 - ♦ Anything caused by humans, they can be intentional or unintentional disasters.
 - ♦ Unintentional could be an employee uses a personal USB stick on a PC at work and spreads malware, just as bad as if an attacker had done it, but the employee were just ignorant, lazy or didn't think it would matter.
 - ♦ Intentional could be malware, terrorism, DOS attacks, hacktivism, phishing, ...
- **Environmental (Not to be confused with natural disasters):**
 - ♦ Anything in our environment, could be power outage/spikes, hardware failures, provider issues, ...
- **Errors and Omissions (Human):**
 - The most common reason for disruptive events are internal employees, often called errors and omissions.
 - They are not intending to harm our organization, but they can inadvertently do so by making mistakes or not following proper security protocols.
 - This could be a mistype, leaving a door unlocked to go outside to smoke or leaving a box of backup tapes somewhere not secure.
 - They often have a minor impact, but if we have issues where they are deemed very common or potentially damaging we can build in controls to mitigate them.
 - We could put a double check in place for the mistype, an alarm on the unlocked door that sounds after being open for 10 seconds, or very clear procedures and controls for the transport of backup tapes.
- **Electrical or Power Problems (Environmental):**
 - Are power outages common in our area?
 - Do we have proper battery and generator backup to sustain our sites for an extended period of time?
 - We want the redundancy of UPS's and generators, they both supply constant and clean power.
 - These should always be in place in data centers, but what about our other buildings?
 - Power fluctuations can damage hardware.
- **Heat (Environmental):**
 - Many data centers are kept too cold, the last decades research has shown it is not needed.
 - Common temperature levels range from 68–77 °F (20–25 °C) - with an allowable range 59–90 °F (15–32 °C).
 - Keeping a Data Center too cold wastes money and raises humidity.
- **Pressure (Environmental):** Keeping positive pressure keeps outside contaminants out.



- **Humidity (Environmental):** Humidity should be kept between 40 and 60% rH (Relative Humidity).
 - Low humidity will cause static electricity and high humidity will corrode metals (electronics).
- **Warfare, Terrorism and Sabotage (Human):**
 - We still see plenty of conventional conflicts and wars, but there is much more happening behind the veil of the internet, hacking for causes, countries, religion and many more reasons.
 - It makes sense to cripple a country's or region's infrastructure if you want to invade or just destabilize that area.
 - This could be for war, trade, influence or many other reasons, everything is so interconnected we can shut down water, electricity or power from across the world.
 - The targets are not always the obvious targets, hospitals, air travel, shipping, production,... are potential targets.
 - **State, Cause or Religious Hacking (Human):**
 - ♦ Common, we often see the attacks happening 9-5 in that time zone, this is a day job.
 - ♦ Approximate 120 countries have been developing ways to use the internet as a weapon to target financial markets, government computer systems and utilities.
 - ♦ Famous attacks: US elections (Russia), Sony websites (N. Korea), Stuxnet (US/Israel), US Office of Personnel Management (China),...
- **Financially Motivated Attackers (Human):**
 - We are seeing more and more financially motivated attacks, they can be both highly skilled or not.
 - The lower skilled ones could be normal phishing attacks, social engineering or vishing, these are often a numbers game, but only a very small percentage needs to pay to make it worth the attack.
 - The ones requiring more skills could be stealing cardholder data, identity theft, fake anti-malware tools, or corporate espionage,...
 - Ransomware is a subtype of financially motivated attacks, it will encrypt a system until a ransom is paid, if not paid the system is unusable, if paid the attacker may send instructions on how to recover the system.
 - Attackers just want the payday, they don't really care from whom.
- **Personnel Shortages (Human/Nature/Environmental):**
 - In our BCP, we also have to ensure that we have redundancy for our personnel and how we handle cases where we have staff shortages.
 - If we have 10% of our staff, how impacted is our organization?
 - This can be caused by natural events (snow, hurricane) but is more commonly caused by the flu or other viruses.
 - **Pandemics:**



- ♦ Organizations should identify critical staff by position not by name, and have it on hand for potential epidemics. <Insert your own COVID-19 work experiences here.>
- **Strikes:**
 - ♦ A work stoppage caused by the mass refusal of employees to work.
 - ♦ Usually takes place in response to employee grievances.
 - ♦ How diminished of a workforce can we have to continue to function?
- **Travel:**
 - ♦ When our employees travel, we need to ensure both they and our data is safe.
 - ♦ That may mean avoiding certain locations, limiting what they bring of hardware and what they can access from the remote location.
 - ♦ If they need laptops/smartphones, we use encryption, device monitoring, VPNs, and all other appropriate measures.

Domain 2: What we covered.

- **BCP (Business Continuity Plan):**
 - The overarching plan, with many subplans.
 - This is the process of creating the long-term strategic business plans, policies, and procedures for continued operation after a disruptive event.
- **DRP (Disaster Recovery Plan):**
 - Focused on our IT systems.
 - How do we recover fast enough in a disaster scenario.
 - DRP has a lifecycle of Mitigation, Preparation, Response and Recovery.
- **Incident Management:**
 - How we monitor and detect security events on our systems, and how we react in those events.